UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

Jane Doe, on behalf of herself and all others similarly situated, Plaintiff, v. The Kroger Co. Defendant.	Case No. 1:23-cv-00750 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

1. Plaintiff Jane Doe at all times relevant herein, has been a patient of The Kroger Co. ("Defendant") by utilizing its online pharmacy, and brings this class action against Defendant in her individual capacity, and on behalf of all others similarly situated ("Class Members" or the "Proposed Class"), and alleges, upon personal knowledge as to her own actions, her counsels' investigation, and upon information and belief as to all other matters, as follows:

2. Plaintiff brings this case to address Defendant's unlawful practice of procuring the interception of and disclosing Plaintiff's and Class Members' confidential Personally Identifiable Information ("PII") and Protected Health Information ("PHI") (collectively referred to as "Private Information") to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook"), without consent.

3. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical

information can have serious consequences, including discrimination in the workplace or denial of insurance coverage. [1]

4. Simply put, if people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

5. A significant part of the need for security and discretion lies in the digital realm. The need for data security (and transparency) is particularly acute when it comes to the rapidly expanding world of digital healthcare as, of all the information the average internet user shares online, health data is some of the most valuable and controversial.[2]

6. Despite professing to value patients' privacy and vowing to protect the confidentiality and security of their private and protected health information, healthcare

---

[1] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022), available at https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited May 1, 2023) ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized."); *see also* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited May 8, 2023).

[2] Protected and highly sensitive medical information collected by healthcare entities includes many categories from intimate details of an individual's conditions, symptoms, diagnoses and treatments to personally identifying information to unique codes which can identify and connect individuals to the collecting entity. *See* Molly Osberg & Dhruv Mehrotral, *The Spooky, Loosely Regulated World of Online Therapy*, JEZEBEL (Feb. 19, 2020), available at https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137 (last visited May 8, 2023).

practices, like Defendant, are collecting, in some instances, "ultra-sensitive personal data" about patients "ranging from those seeking information about their reproductive rights and options, those seeking information regarding their addictions and . . . those seeking mental health counseling."[3]

7. And, while mobile health options have been celebrated as a way to expand treatment options, the tangible, real-world implications and potential for abuse is staggering:

> [T]he sensitive information people share during treatment for substance use disorders could easily impact their employment status, ability to get a home, custody of their children, and even their freedom. Health care providers and lawmakers recognized long ago that the potential threat of losing so much would deter people from getting life-saving help and set up strict laws to protect those who do seek treatment. ***Now, experts worry that data collected on telehealth sites could bring about the harm [the law] was designed to prevent and more, even inadvertently***.[4]

8. Recognizing these incontrovertible facts and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the United States Department of Health and Human Services ("HHS") has established "Standards for Privacy of Individually Identifiable Health Information" (also

---

[3] Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, REVEAL (June 15, 2022), available at https://revealnews.org/article/facebook-data-abortion-crisis-pregnancy-center/ (noting that such "personal data can be used in a number of ways. The centers can deliver targeted advertising, on Facebook or elsewhere, aimed at deterring an individual from getting an abortion. It can be used to build anti-abortion ad campaigns – and spread misinformation about reproductive health – targeted at people with similar demographics and interests. And, in the worst-case scenario now contemplated by privacy experts, that digital trail might even be used as evidence against abortion seekers in states where the procedure is outlawed") (last visited May 10, 2023).

[4] *Id.* (emphasis added).

known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

9. Healthcare organizations regulated under HIPAA may use third-party tracking tools, such as Google Analytics or Meta Pixel, only in a limited way, to perform analysis on data key to operations:

> To be sure, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the unlawful transmission of such protected information violates HIPAA's Privacy Rule: Regulated [E]ntities [those to which HIPAA applies] are not permitted to use [T]racking [T]echnologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[5]

10. In addition, Ohio Revised Code § 2933 provides for a civil cause of action for any person whose wire, oral, or electronic communications are intercepted, disclosed, or intentionally used in violation of §§ 2933.51 to 2933.66 of the Revised Code. Available relief for such violations may include the preliminary and other equitable or declaratory relief that is appropriate; Whichever of the following is greater: (1) Liquidated damages

[5] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited May 10, 2023) (emphasis added).

computed at a rate of two hundred dollars per day for each day of violation or (2) liquidated damages of ten thousand dollars, whichever is greater; The sum of actual damages suffered by the plaintiff and the profits, if any, made as a result of the violation by the person or entity that engaged in the violation; Punitive damages, if appropriate; and reasonable attorney's fees and other litigation expenses that are reasonably incurred in bringing the civil action.

11. To establish liability under Ohio Revised Code § 2933, Plaintiff and putative Ohio Class Members need only establish that the Defendant caused a wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities.

12. Defendant owns and controls www.kroger.com/health/pharmacy ("Defendant's Website" or the "Website"), which it encourages patients to use for booking medical appointments, scheduling consultations, locating facilities, searching varieties of procedures and treatment options, and more.

13. Defendant represents that it values the privacy of its patients and those who enquire about services advertises to its prospective and current patients that its online functionality is a secure and private means of interacting with Defendant.

14. Plaintiff and other Class Members who used Defendant's Website understandably thought they were communicating only with a trusted medical provider. Unbeknownst to Plaintiff and Class Members, however, Defendant had embedded the Facebook Tracking Pixel (the "Pixel" or "Facebook Pixel") into its Website, surreptitiously

forcing Plaintiff and Class Members to transmit their Private Information to Facebook without consent.

15. Operating as designed and as implemented by Defendant, the Pixel allows the Private Information that Plaintiff and Class Members submit to Defendant to be unlawfully disclosed to Facebook alongside the individual's unique and persistent Facebook ID ("FID").[6]

16. A pixel is a piece of code that "tracks the people and [the] type of actions they take"[7] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), among other things.

17. The user's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Facebook Pixel is thus customizable and programmable, meaning that the website owner controls which of its webpages contain the Pixel and which events are tracked and transmitted to Facebook.

18. When a website user visits a webpage containing Pixels, their device is commandeered, and their communications are surreptitiously duplicated and transmitted

[6] The Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited April 18, 2023).

[7] Facebook, *Retargeting*, https://www.facebook.com/business/goals/retargeting (last visited April 18, 2023)

to third parties. Stated differently, Defendant's Website and Pixel purposely altered patients' web browsers, forcing them to duplicate and redirect communications to third-party web servers.

19. The information sent to third parties included the Private Information that Plaintiff and Class Members submitted to Defendant's Website related to their past, present, or future health conditions or elective interests, including, for example, the type and date of a medical appointment and physician. Such Private Information would allow the third party (*e.g.*, Facebook or Google) to know that a specific patient was seeking confidential care and the type of medical care being sought. This disclosure would also allow a third party to reasonably infer that a specific patient was being treated due to a specific type of medical condition such as cancer, obesity, or gynecomastia.

20. Simply put, by installing the Facebook Pixel into its Website, Defendant effectively planted a bug on Plaintiff and Class Members' web browsers and compelled them to disclose their communications with Defendant to Facebook.

21. In addition to the Facebook Pixel, Defendant also installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on its Website servers.[8]

22. Unlike the Facebook Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does

[8] "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Jan. 25, 2023).

not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including their Private Information, then records and stores that information on the website owner's servers, to then in turn transmit the data to Facebook from the website owner's servers.[9, 10] Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[11]

23. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Pixel from sending website users' Private Information to Facebook directly.

24. Defendant utilized the Pixel and CAPI data for marketing purposes in an effort to bolster its profits. The Facebook Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff's and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

---

[9] https://revealbot.com/blog/facebook-conversions-api/ (last visited Jan. 24, 2023).

[10] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels.", https://developers.facebook.com/docs/marketing-api/conversions-api (last visited Jan. 27, 2023).

[11] https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Jan. 28, 2023).

25. The information disclosed in this way by Defendant allows a third party (*e.g.*, Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers who geotarget Plaintiff's and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and CAPI.

26. The Office for Civil Rights (OCR) at HHS has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("Regulated Entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online Tracking Technologies ("Tracking Technologies").[12] The Bulletin expressly provides that "Regulated [E]ntities are not permitted to use [T]racking [T]echnologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules." In other words, HHS has expressly stated that entities like Defendant that implement the Facebook Pixel have violated HIPAA Rules.

27. The HHS Bulletin further warns that:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care

[12] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Feb. 20, 2023).

> professionals, and where an individual seeks medical treatment. While it has always been true that [R]egulated [E]ntities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of [T]racking [T]echnologies collecting sensitive information, now more than ever, it is critical for [R]egulated [E]ntities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [13]

28. Healthcare patients simply do not anticipate that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party – let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue – without the patients' consent. Neither Plaintiff nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook.

29. Despite willfully and intentionally incorporating the Facebook Pixel and CAPI into its Website and servers, Defendant has never disclosed to Plaintiff or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook. Plaintiff and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook as they communicated with their healthcare provider via the Website or stored on Defendant's servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes.

[13] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Apr. 18, 2023).

30. Defendant breached its statutory and common law obligations to Plaintiff and Class Members by, inter alia,: (i) failing to adequately review its marketing programs and web-based technology to ensure the Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the written consent of Plaintiff and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Facebook Pixels; (v) failing to warn Plaintiff and Class Members; and (vi) otherwise failing to design, and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

31. As a result of Defendant's conduct, Plaintiff and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of the bargain, (iii) diminution of value of the Private Information, (iv) statutory damages, and (v) the continued and ongoing risk to their Private Information.

32. Plaintiff seeks to remedy these harms and brings causes of action for (i) invasion of privacy; (ii) violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(1) –unauthorized interception, use, and disclosure; (iii) breach of confidence; (iv) breach of implied contract; (v) negligence; and (vi) breach of fiduciary duty.

PARTIES

33. Plaintiff Jane Doe is a natural person and citizen of the State of Ohio and resides within the County of Franklin where she intends to remain.

34. Defendant is a public company with its principal place of business at 1014 Vine St., Cincinnati, Ohio 45202 with its Registered Agent as Corporation Service Company located at 3366 Riverside Drive, Suite 103, Upper Arlington, OH 43221. Defendant is one of the largest supermarket operators in the United States. Kroger employs approximately 465,000 individuals nationwide and generated annual revenue in the amount of $3.477 billion in 2022.

JURISDCTION & VENUE

35. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this case is brought as a class action where the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendant.

36. This Court has federal question jurisdiction under 29 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (28 U.S.C. § 2511, *et seq.*).

37. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

38. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

A. *Background: Underlying Technology Employed by Defendant for the Purpose of Disclosing Plaintiff and Class Members' Private Information to Facebook*

39. Defendant purposely installed the Pixel and Conversions API tools on many of its webpages within its Website and programmed those webpages to surreptitiously share its patients' private and protected communications with Facebook, including communications that contain Plaintiff's and Class Members' Private Information.

40. Defendant uses the Website to connect Plaintiff and Class Members to Defendant's digital healthcare platforms with the goal of increasing profitability.

41. In order to understand Defendant's unlawful data-sharing practices, it is important first to understand basic web design and tracking tools.

B. *Facebook's Business Tools and the Pixel*

42. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[14]

43. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

[14] Facebook, *Meta Reports Fourth Quarter and Full Year 2021 Results* , https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Apr. 5, 2023).

44. Facebook's Business Tools, including the Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

45. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[15] Businesses that want to target customers and advertise their services, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[16]

46. One such Business Tool is the Pixel which "tracks the people and type of actions they take."[17] When a user accesses a webpage that is hosting the Pixel, the communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook—traveling from the user's browser to Facebook's server.

---

[15] Facebook, *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited Mar. 1, 2023); *see* Facebook, *Facebook Pixel, Accurate Event Tracking, Advanced*, https://developers.facebook.com/docs/facebook-pixel/advanced/ (last visited Apr. 5, 2023); *see also* Facebook, *Best Practices for Facebook Pixel Setup*, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; Facebook, *App Events API*, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Apr. 5, 2023).

[16] Facebook, *About Standard and Custom Website Events*, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* Facebook, *App Events API*, *supra*.

[17] Facebook, *Retargeting*, https://www.facebook.com/business/goals/retargeting.

47. Notably, this transmission only occurs on webpages that contain the Pixel. Thus, Plaintiff's and Class Member's Private Information would not have been disclosed to Facebook via the Pixel but for Defendant's decisions to install the Pixel on its Website.

48. Similarly, Plaintiff's and Class Member's Private Information would not have been disclosed to Facebook via Conversions API but for Defendant's decision to install and implement that tool.

49. By installing and implementing both tools, Defendant caused Plaintiff's and Class Member's communications to be intercepted and transmitted to Facebook via the Pixel, and it caused a second improper disclosure of that information via Conversions API.

50. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via certain webpages.

C. *Defendant's Method of Transmitting Plaintiff's and Class Members' Private Information via the Tracking Pixel and/or Conversions API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Pixel*

51. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

52. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

53. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses. Any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF for filing a motion to a court)
- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.[18]

54. A patient's HTTP Request essentially asks the Defendant's Website to retrieve certain information. The HTTP Response sends the requested information in the

[18] One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Website.

55. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

56. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When patients visit Defendant's website via an HTTP Request to Defendant's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel. Thus, Defendant is in essence handing patients a tapped phone, and once the Webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook and Google.

57. Third parties, like Facebook, place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the patient associated with the Personal Information intercepted.

58. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on

gathering Personal Information, like Facebook, implement workarounds that savvy users cannot evade. Facebook's workaround, for example, is called Conversions API. Conversions API is an effective workaround because it does the transmission from their own servers and does not rely on the User's web browsers. Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]." Thus, the communications between patients and Defendant, which are necessary to use Defendant's Website, are actually received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

59. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like Conversions API without access to the host server, companies like Facebook instruct Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[19] Thus, it is reasonable to infer that Facebook's customers who implement the Facebook Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround.

60. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user's

[19] *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Jan. 23, 2023).

communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner (*i.e.*, to bolster profits).

61. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

62. In this case, Defendant employed the Tracking Pixel and Conversions API to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Facebook.

63. The Facebook Tracking Pixel is embedded in Defendant's Source Code contained in its HTTP Response. The Pixel, programmed to automatically track and transmit the patient's communications with Defendant's Website to Facebook, executes instructions that effectively open a hidden spying window into the patient's browser through which Facebook can intercept the visitor's data, actions, and communications with Defendant.[20]

64. Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and to send those communications to Facebook. These transmissions occur contemporaneously, invisibly, and without the patient's knowledge.

[20] When used in the context of a screen or visual display, a "pixel" is the smallest unit in such a digital display. An image or video on a device's screen can be made up of millions of individual pixels. The Facebook Pixel is a tiny image file that is so small as to be invisible to website users. It is purposefully designed and camouflaged in this manner so that website users remain unaware of it.

65. Thus, without its patients' consent, Defendant has effectively used its source code to commandeer and "bug" or "tap" it patients' computing devices, allowing Facebook and other third parties to listen in on all of their communications with Defendant and thereby intercept those communications, including Private Information.

66. Consequently, when Plaintiff and Class Members visit Defendant's website and communicate their Private Information, including, but not limited to: selecting desired procedures and their specific areas, button clicks to navigate the Website, viewing information on specified procedures, accessing patient resources including information for pre and post op, financials, insurance, hospital packages, pain packages, and the sites HIPAA and Privacy Policy pages, to third parties like Facebook receive the information.

D. *Defendant Disclosed Plaintiff's and Class Members' Private Information to Facebook Using the Pixel and/or Conversions API Tracking Practices*

67. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel and Conversions API ("First Party Cookies") on its Website and servers to secretly track patients by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties and obligations.[21]

68. Defendant's Pixel has its own unique identifier (represented as id=126589911409162) which can be used to identify which of Defendant's webpages contain the Pixel.

[21] *Id.*

69. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs.[22] However, Defendant's Website do not rely on the Pixel in order to function.

70. While seeking and using Defendant's services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendant via its Website.

71. Plaintiff and Class Members were not aware that their Private Information would be shared with Facebook as it was communicated to Defendant because, amongst other things, Defendant did not disclose this fact.

72. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to Facebook, nor did they intend for Facebook to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

73. Defendant's Pixel and First Party Cookies sent non-public Private Information to Facebook, including but not limited to Plaintiff's and Class Members': (1) status as medical patients; (2) health conditions; (3) prescriptions; and (4) other medical information.

74. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside Plaintiff's and Class Members' Facebook ID (c_user cookie or "FID"), thereby allowing individual patients' communications with Defendant, and the Private

[22] *Id.*

Information contained in those communications, to be linked to their unique Facebook accounts and therefore their identity.[23]

75. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including location, pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

76. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (*i.e.*, the Facebook Pixel and First Party Cookies) that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Facebook—an unauthorized third-party; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

E. *Facebook Exploited and Used Plaintiff's and Class Members' Private Information*

77. Unsurprisingly, Facebook does not offer its Pixel to companies like Defendant solely for Defendant's benefit. "Data is the New Oil of the Digital Economy,"[24]

[23] Defendant's Website track and transmit data via first-party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

[24] *Data is the New Oil of the Digital Economy*, https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last visited November 13, 2023).

and Facebook has built its more-than $300 billion market capitalization on mining and using that 'digital' oil. Thus, the large volumes of personal and sensitive health or medical-related data Defendant provided to Facebook are actively viewed, examined, analyzed, curated, and put to use by the company. Facebook acquires the raw data to transform it into a monetizable commodity, just as an oil company acquires crude oil to transform it into gasoline. Indeed, Facebook offers the Pixel free of charge[25] and the price that Defendant pays for the Pixel is the data that it allows Facebook to collect.

78. Facebook sells advertising space by emphasizing its ability to target users.[26] Facebook is especially effective at targeting users because it surveils user activity both on and off its site (with the help of companies like Defendant).[27] This allows Facebook to make inferences about users beyond what they explicitly disclose, including their "interests," "behavior," and "connections."[28] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[29]

---

[25] *Facebook Pixel: What It Is and Why You Need It*, https://seodigitalgroup.com/facebook-pixel/ (last visited Nov. 13, 2023).

[26] *Facebook, Why Advertise on Facebook*, https://www.facebook.com/business/help/205029060038706 (last visited Nov. 13, 2023).

27 *Facebook, About Facebook Pixel*, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Nov. 13, 2023).

[28] *Facebook, Ad Targeting: Help your ads find the people who will love your business*, https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 13, 2023).

[29] *Facebook, Easier, More Effective Ways to Reach the Right People on Facebook*, https://www.facebook.com/business/news/Core-Audiences (last visited Nov. 13, 2023).

79. Advertisers can also build "Custom Audiences,"[30] which helps them reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[31] With Custom Audiences, advertisers can target existing customers directly. They can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[32] Unlike Core Audiences, Custom Audiences and Lookalike Audiences are only available if the advertiser has sent its underlying data to Facebook. This data can be supplied to Facebook by manually uploading contact information for customers or by utilizing Facebook's "Business Tools" like the Pixel and Conversions API.[33]

80. Facebook does not merely collect information gathered by the Pixel and store it for safekeeping on its servers without ever viewing or accessing the information. Instead, in accordance with the purpose of the Pixel to allow Facebook to create Core, Custom, and Lookalike Audiences for advertising and marketing purposes, Facebook viewed,

---

[30] *Facebook, About Custom Audiences*, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited Nov. 13, 2023).

[31] *Facebook, Ad Targeting, Help your ads find the people who will love your business*, https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 13, 2023).

[32] *Facebook, About Lookalike Audiences*, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited Nov. 13, 2023).

[33] *Facebook, Create a Customer List Custom Audience*, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited Nov. 13, 2023); *Facebook, Create a Website Custom Audience*, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited Nov. 13, 2023).

processed, and analyzed Plaintiff's and Class Members' confidential Private Information. Upon information and belief, such viewing, processing, and analyzing was performed by computers and/or algorithms programmed and designed by Facebook employees at the direction and behest of Facebook.

81. Facebook receives over 4 petabytes[34] of information every day and must rely on analytical tools designed to view, categorize, and extrapolate the data to augment human effort.[35] This process is known as "data ingestion" and allows "businesses to manage and make sense of large amounts of data."[36]

82. By using data ingestion tools, Facebook is able to rapidly translate the information it receives from the Pixel in order to display relevant ads to consumers. For example, if a consumer visits a retailer's webpage and places an item in their shopping cart without purchasing it, the next time the shopper visits Facebook, an ad for that item will appear on the shopper's Facebook page.[37] This evidences that Facebook views and categorizes data as they are received from the Pixel.

---

[34] A petabyte is equal to one million gigabytes (1,000,000 GB).

[35] *How does [F]acbook handle the 4+ petabyte of data generate per day? Cambridge Analytica – [F]acebook data scandal.,* https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4 (last visited Nov. 13, 2023). Facebook employees would not be able to view each piece of data individually – millions of them per second – without the aid of technology. Just as a microscope or telescope allows the user to see very small or very distant objects by zooming in, however, Facebook's big data management software allows the company to see all of this data at once by zooming out.

[36] *Facebook database [Updated] – A thorough insight into the databases used @Facebook,* https://scaleyourapp.com/what-database-does-facebook-use-a-1000-feet-deep-dive/ (last visited Nov. 13, 2023). Facebook uses ODS, Scuba, and Hive to manage its massive data stores. These technologies are not traditional databases; they are specialized databases for big data designed to process data specifically for analysis—"such as [viewing] hidden patterns, correlations, market trends and customer preferences."

[37] *A Complete Guide to Facebook Tracking for Beginners,* https://www.oberlo.com/blog/facebook-pixel (last visited Nov. 13, 2023).

83. Moreover, even if Facebook eventually deletes or anonymizes Private Information that it receives, it must first view that information in order to identify it as containing Private Information suitable for removal. Accordingly, there is a breach of confidentiality the instant the information is disclosed or received without authorization. As described by the HHS Bulletin:

> It is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place and requires that there is an applicable Privacy Rule permission for disclosure.[38]

F. *Plaintiff Jane Doe's Experiences*

84. Plaintiff Jane Doe entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Doe disclosed her Private Information to Defendant.

85. Plaintiff Doe also maintains and regularly uses her Facebook and Instagram accounts, primarily from her mobile phone.

86. Plaintiff Doe accessed Defendant's Website via her mobile phone to receive healthcare services from Defendant, availing herself of the healthcare resources and services provided by Defendant to its customers.

---

[38] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business* Associates, U.S. Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (emphasis in original) (last visited Nov. 13, 2023).

87. Plaintiff Doe reasonably expected that her communications with Defendant via the website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

88. Plaintiff Doe provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

89. Indeed, Plaintiff Doe is extraordinarily protective of her Private Information, using multi-factor authentication to protect her online accounts, thoroughly destroying unnecessary physical documents with Private Information, and disabling certain features on her devices that go to far in tracking or monitoring her activity, life, or behavior.

90. As described herein, Defendant worked along with Facebook and its parent company (Meta) to intercept Plaintiff Doe's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff Doe's knowledge, consent, or express written authorization.

91. Defendant transmitted to Facebook Plaintiff Doe's Private Information, including her name, address, phone number, date of birth, and email address, along with the details (including time, place, and purpose) of medical appointments Plaintiff Doe scheduled with Defendant via Defendant's Website.

92. For example, Plaintiff Doe has used Defendant's Website annually during the relevant time period to schedule vaccine appointments and refill prescriptions. Defendant has transmitted to Facebook the dates and locations of these appointments, as well as the purpose of those appointments.

93. By doing so without Plaintiff Doe's consent, Defendant breached Plaintiff Doe's right to privacy and unlawfully disclosed Plaintiff's Private Information.

94. Plaintiff Doe suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, (iii) loss of benefit of the bargain, (iv) diminution of value of her Private Information, (v) statutory damages and (v) the continued and ongoing risk to her Private Information.

95. Plaintiff Doe has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future unauthorized disclosure.

G. *Defendant's Conduct Is Unlawful and Violated Industry Norms*

i. Defendant Violated HIPAA Standards

96. Defendant is not merely a source of medical information, such as the various subject matter clearinghouses available on the internet but is a healthcare provider. In fact, Defendant cites the number of board certifications and professional designations associated with its practice throughout its website.

97. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[39]

[39] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

98. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

99. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[40]

100. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

101. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

[40] HHS.gov, HIPAA For Professionals (last visited Apr. 12, 2023), https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html.

102. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

> a. Names;
>
> ***
>
> H. Medical record numbers;
>
> ***
>
> J. Account numbers;
>
> ***
>
> M. Device identifiers and serial numbers;
>
> N. Web Universal Resource Locators (URLs);
>
> O. Internet Protocol (IP) address numbers; … and
>
> R. Any other unique identifying number, characteristic, or code…;and"
>
> The covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 160.514.

103. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of

protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

104. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6.

105. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

106. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both."

107. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[41]

108. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added).[42]

109. As alleged above, there is an HHS Bulletin that highlights the obligations of "[R]egulated [E]ntities," which are HIPAA-covered entities and business associates, when using [T]racking [T]echnologies.[43]

---

[41] *Guidance Regarding Methods for De-identificaiton of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,* https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 13, 2023).

[42] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Nov. 13, 2023)

[43] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

110. The Bulletin expressly provides that "[r]egulated entities are not permitted to use [T]racking [T]echnologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

111. Defendant's actions violated HIPAA Rules per this Bulletin.

ii. Defendant Violated Industry Standards

112. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient relationship.

113. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

114. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)

115. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-

(last visited Nov. 13, 2023).

> making capacity about the purposes for which access would be granted.

116. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must…:(c) release patient information only in keeping ethics guidelines for confidentiality.

H. *Plaintiff's and Class Members' Expectation of Privacy*

117. Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

118. Indeed, at all times when Plaintiff and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

119. Plaintiff and Class Members would not have used Defendant's Website, would not have provided their Private Information to Defendant, and would not have paid for Defendant's healthcare services, or would have paid less for them, had they known that Defendant would disclose their Private Information to third parties.

I. *IP Addresses Are Personally Identifiable Information*

120. On information and belief, through the use of the Facebook Pixel on Defendant's Website, Defendant also disclosed and otherwise assisted Facebook with intercepting Plaintiff's and Class Members' Computer IP addresses.

121. An IP address is a number that identifies the address of a device connected to the Internet.

122. IP addresses are used to identify and route communications on the Internet.

123. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

124. Facebook tracks every IP address ever associated with a Facebook user.

125. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

126. Under HIPAA, an IP address is considered personally identifiable information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).
- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

127. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

J. *Defendant Was Enriched and Benefitted from the Use of The Pixel and*

Unauthorized Disclosures

128. The primary motivation and a determining factor in Defendant's interception and disclosure of Plaintiff's and Class Members' Private Information was to commit criminal and tortious acts in violation of federal and state laws as alleged herein, namely, the use of patient data for advertising in the absence of express written consent. Defendant's further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was in violation of HIPAA and an invasion of privacy. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on its platform.

129. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

130. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients to use its services. Defendant did so through use of the intercepted patient data it obtained, procured, and/or disclosed in the absence of express written consent.

131. By utilizing the Pixel, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby benefitting Defendant while invading the privacy of Plaintiff and Class Members and violating their rights under federal and Pennsylvania law.

K. ***Plaintiff's and Class Members' Private Information Had Financial Value***

132. Plaintiff's data and Private Information has economic value. Facebook regularly uses data that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences and then sells that information to advertising clients.

133. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

134. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[44]

135. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[45]

---

[44] *See How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, Time Magazine, https://time.com/4588104/medical-data-industry/ (last visited Nov. 13, 2023).

[45] *See Hospital execs say they are getting flooded with requests for your health data.* CNBC https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Nov. 13, 2023).

TOLLING

136. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that his PII and PHI was intercepted and unlawfully disclosed to Facebook because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

137. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

138. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the United States who are, or were, patients of Defendant or any of its affiliates, who used Defendant's Website and had their Private Information disclosed to a third party without authorization.

139. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

140. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

141. **Numerosity**, Fed R. Civ. P. 23(a)(1). The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are likely

thousands of individuals whose PII and PHI may have been improperly disclosed to Facebook, and the Class is identifiable within Defendant's records.

142. **Commonality**, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

d. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

e. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

g. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct; and

h. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their Private Information.

143. **Typicality**, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

144. **Adequacy**, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

145. **Superiority and Manageability**, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those

Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

146. **Policies Generally Applicable to the Class**. Fed. R. Civ. P. 23(b)(2). This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

147. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

148. The litigation of the claims is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

149. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

150. Unless a class-wide injunction is issued, Defendant may continue disclosing the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

151. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

152. **Issue Certification**, Fed. R. Civ. P. 23(c)(4). Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to, the following:

a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

f. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

153. Plaintiff incorporates all prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

227. The Private Information of Plaintiff and Class Members consists of private and confidential facts and information that were never intended to be shared beyond private communications.

228. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

229. Defendant owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

230. Defendant owed a duty to Plaintiff and Class Members not to give publicity to their private lives to Facebook and, by extension, other third-party advertisers and businesses who purchased Facebook's advertising services.

231. Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information to Facebook, a third-party social media and marketing giant, is highly offensive to a reasonable person.

232. Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Private Information constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

233. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiff's and Class Members' privacy because Defendant exceeded its authorization to access Plaintiff's and Class Members' information and facilitated Facebook's simultaneous eavesdropping and wiretapping of confidential communications.

234. Defendant failed to protect Plaintiff's and Class Members' Private Information and acted knowingly when it installed the Pixel onto its Website because the

purpose of the Pixel is to track and disseminate individual's communications with the Website for the purpose of marketing and advertising.

235. Because Defendant intentionally and willfully incorporated the Facebook Pixel into its Website and encouraged patients to use that Website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiff and Class Members.

236. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiff and the Class Members was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

237. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, plus prejudgment interest, and costs.

238. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant and still in the possession of Facebook and other third parties and the wrongful disclosure of the information cannot be undone.

239. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook who on information and belief continues to possess and utilize that information.

240. Plaintiff, on behalf of herself and Class Members, further seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT II
VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA") 18 U.S.C. § 2511(1) *ET SEQ.*
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(ON BEHALF OF PLAINTIFF AND THE CLASS)

241. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

242. The ECPA protects both sending and receipt of communications.

243. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

244. The transmissions of Plaintiff's Private Information to Defendant via Defendant' Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

245. The transmissions of Plaintiff's Private Information to medical professionals qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(2).

246. **Electronic Communications**. The transmission of Private Information between Plaintiff and Class Members and Defendant via its Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio,

electromagnetic, photoelectronic or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

247. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

248. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

249. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendant's web-servers; and

d. The Pixel deployed by Defendant to effectuate the sending and acquisition of patient communications.

250. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the Tracking Pixel imbedded and ran on its Website, contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiff's and Class Members' electronic communications to third parties, including

Facebook and Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

251. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the Tracking Pixel imbedded and run on its Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiff's and Class Members' electronic communications, for purposes other than providing health care services to Plaintiff and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

252. Whenever Plaintiff and Class Members interacted with Defendant's Website, Defendant, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally redirected the contents of Plaintiff's and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook and Google.

253. Defendant's intercepted communications include, but are not limited to, the contents of communications to/from Plaintiff and Class Members' regarding their Private Information, treatment, medication, and scheduling.

254. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the

interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

255. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

256. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiff's and Class Members' Private Information for financial gain.

257. Defendant was not acting under color of law to intercept Plaintiff's and Class Members' wire or electronic communication.

258. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the Pixel tracking code.

259. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

260. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State.

261. The ECPA provides that a "party to the communication" may be liable where a "communication is intercepted for the purpose of committing any criminal or tortious act

in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

262. Defendant is a "party to the communication" with respect to patient communications. However, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

263. Defendant's acquisition of patient communications that were used and disclosed to

Facebook and Google was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and Pennsylvania, including.

a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;

b. Violation of Ohio Revised Code § 2933; and

c. Invasion of Privacy.

264. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person … without authorization" from the patient.

265. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

266. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it:

a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and

b. Disclosed individually identifiable health information to Facebook and Google without patient authorization.

267. Defendant's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant's use of the Facebook and Google source code was for Defendant's commercial advantage to increase revenue from existing patients and gain new patients.

268. A patient has the right to every consideration of her privacy concerning her own medical care program. In addition, a patient has the right to have all records pertaining to her medical care treated as confidential except as otherwise provided by law or third-party contractual arrangements.

269. Defendant violated of Ohio Revised Code § 2933 by disclosing Plaintiff's and Class Members' Private Information to third parties without proper authorization or consent.

270. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiff's and Class Members' communications about their individually-identifiable PHI on its Website, because it used its participation in these communications to improperly share Plaintiff's and Class Members' individually-identifiable PHI with Facebook and Google, third-parties that did not participate in these communications, that Plaintiff and Class Members did not know were receiving their individually-identifiable PHI, and that Plaintiff and Class Members did not consent to receive this information.

271. Defendant accessed, obtained, and disclosed Plaintiff's and Class Members' Private Information for the purpose of committing the crimes and torts described herein because it would not have been able to obtain the information or the marketing services if it had complied with the law.

272. As such, Defendants cannot viably claim any exception to ECPA liability.

273. Plaintiff and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their individually-identifiable PHI (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiff and the Class Members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiff's and Class Members' individually identifiable PHI without providing any value or benefit to Plaintiff or the Class Members;

c. Defendant received substantial, quantifiable value from its use of Plaintiff's and Class Members' individually-identifiable PHI, such as understanding how people use its website and determining what ads people see on its website, without providing any value or benefit to Plaintiffs or the Class Members;

d. Defendant has failed to provide Plaintiff and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their PHI; and

e. The diminution in value of Plaintiff's and Class Members' Private Information and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiff and Class Members intended to remain private no longer private.

274. As a result of Defendant's violation of the ECPA, Plaintiffs are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT III
BREACH OF CONFIDENCE
(ON BEHALF OF PLAINTIFF AND THE CLASS)

275. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

276. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

277. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website, which were further buttressed by Defendant's express promises in its privacy policy.

278. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Pixel and Conversions API to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant, including Private Information and the contents of such information.

279. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

280. The third-party recipients included, but may not be limited to, Facebook. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

281. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Class members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiff and Class members intended to remain private is no longer private;

b. Plaintiff and Class members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

d. General damages for invasion of their rights in an amount to be determined by a jury;

e. Nominal damages for each independent violation;

f. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without compensation for such data;

g. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

h. Defendant's actions diminished the value of Plaintiff's and Class Members' Private Information; and

i. Defendant's actions violated the property rights Plaintiff and Class members have in their Private Information.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

282. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

283. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiff and Class Members provided their Private Information and compensation for their medical care.

284. When Plaintiff and Class Members provided their Private Information to Defendant, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

285. Plaintiff and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

286. Plaintiff and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

287. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' Private Information without consent to third parties for commercial purposes.

288. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiff and Class Members sustained damages as alleged herein, including but not limited to the loss of the benefit of their bargain and diminution in value of Private Information.

289. Defendant's breaches of implied contract were a direct and proximate cause of several injuries suffered by Plaintiff and Class Members, including, but not limited to, losses of privacy, interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains with Defendant. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract. In the alternative, Plaintiff and Class Members seek nominal damages.

COUNT V
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

290. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

291. This claim is brought in the alternative to Breach of Confidence.

292. Defendant owed Plaintiff and Class Members a duty to keep their Private Information completely confidential, and to safeguard sensitive personal and medical information.

293. Plaintiff and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

294. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Tracking Tools to disclose and transmit to third parties Plaintiff's and Class Members' communications with Defendant, including Private Information and the contents of such information.

295. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization, and were unprivileged.

296. Defendant's negligence was a direct and proximate cause of several injuries suffered by Plaintiff and Class Members, including, but not limited to, losses of privacy, interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains with Defendant. Plaintiff and Class Members seek

compensatory damages in an amount to be proved at trial. In the alternative, Plaintiff and Class Members seek nominal damages.

COUNT VI
BREACH OF FIDUCIARY DUTY
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

297. Plaintiff incorporates the prior allegations as if fully set forth herein and brings this Count individually and on behalf of the proposed Class.

298. This claim is brought in the alternative to breach of confidence (Biddle).

299. Defendant has a fiduciary duty to act primarily for the benefit of its patients, including Plaintiff and Class Members by: (1) safeguarding Plaintiff's and Class Members' Private Information; (2) timely notifying Plaintiff and Class Members of disclosure of their Private Information to unauthorized third parties; and (3) maintaining complete and accurate records of what patient information (and where) Defendant did and does store and disclose.

300. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to protect and/or intentionally disclosing Plaintiff's and Class Members' Private Information to third parties without authorization or consent.

301. Defendant's breach of fiduciary duty is evidenced by its failure to comply with federal and state privacy regulations, including:

a. By failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

b. By failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

c. By failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4);

d. By failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiff's and Class Members' PHI;

e. By failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. By failing to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in violation of 45 C.F.R. § 164.312(e)(1);

g. By impermissibly and improperly using and disclosing Private Information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq., 45 C.F.R. § 164.508, et seq., and R.C. 3798.04, et seq.;

h. By failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as

necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. By failing to comply with R.C. 3798.04 regarding the use or disclosure of protected health information

302. Defendant's breaches of fiduciary duty were a direct and proximate cause of several injuries suffered by Plaintiff and Class Members, including, but not limited to, losses of privacy, interference with confidential relationships, diminished value of Private Information, and the lost benefit of their bargains. Plaintiff and Class Members seek compensatory damages in an amount to be proved at trial. In the alternative, Plaintiff and Class Members seek nominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiff and Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members:

D. For an award of damages, including, but not limited to, actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Respectfully Submitted,

Dated: November 13, 2023

/s/ Joseph M. Lyon
Joseph M. Lyon (OH Bar #76050)
Kevin M. Cox (OH Bar #99584)
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Telephone: (513) 381-2333
Facsimile: (513) 766-9011
jlyon@thelyonfirm.com
kcox@thelyonfirm.com

Philip J. Krzeski (OH BAR #0095713)
Bryan L. Bleichner (*Pro Hac Vice* forthcoming)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2940
bbleichner@chestnutcambronne.com

pkrzeski@chestnutcambronne.com

ATTORNEYS FOR PLAINTIFF JANE DOE AND THE PROPOSED CLASS